УДК 681.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

Приймак М.В.
Национальный университет обороны Украины имени Ивана Черняховского

В статье проведен анализ методических подходов к оценке эффективного обеспечения безопасности объектов информационной инфраструктуры государства (ИИГ). Предложено описание формализованной модели функционирования объектов информационной инфраструктуры государства. Рассмотрены общие принципы определения критических объектов инфраструктуры. Описана система мероприятий по нейтрализации (минимизации) угроз объектам ИИГ и величины их возможного ущерба. Предложены задачи обеспечения безопасности объектов ИИГ.
Ключевые слова: информационная инфраструктура государства, критический объект, информационная безопасность.

Постановка проблемы. В связи с тем, что Украина де-факто находится в состоянии вооружённого конфликта, причём на своей территории, приходится рассматривать информационную сферу именно как ещё одно пространство противоборства. Объектами опасного

информационного воздействия и, следовательно, информационной безопасности являются множество объектов информационной инфраструктуры государства (ИИГ), как государственных, так и частных.

События последних лет, такие как атаки на энергетические объекты Украины с помощью программы BlackEnergy, применение кибероружия (Stuxnet и др.), физический захват объектов [3], остро ставят вопрос о создании эффективной государственной системы защиты (координации защиты) критических объектов информационной структуры от деструктивных физических и информационных воздействий.

Анализ последних исследований и публикаций. Анализ источников [7; 12; 16] показал, что общепринятые подходы по определению критических (наиболее важных) объектов ИИГ, методы, которые определяют, возможные мероприятия и задачи по их защите находятся в стадии постоянного совершенствования вследствие увеличения и изменения угроз, воздействующих на эти объекты.

Выделение нерешенных ранее частей общей проблемы. Это порождает необходимость в определении сущности критических объектов информационной инфраструктуры государства, которые будут учитывать чрезмерную уязвимость всех без исключения каналов связи и медиаконтента, основанных преимущественно на использовании наземной инфраструктуры [4].

Управление безопасностью объектов информационной инфраструктуры государства занимает всё более значимое место в функционировании государства [5; 18], применяющего современные технологии сбора, хранения и обработки информации. Данный процесс основывается на периодическом проведении анализа информационных рисков, который позволяет своевременно выявлять угрозы информационной безопасности, уязвимости информационной системы, внедрять соответствующие мероприятия по их нейтрализации и, как следствие, постоянно отслеживать состояние информационной безопасности в государстве, учитывая новые угрозы и уязвимости.

В настоящее время используется множество разнообразных методик анализа информационных рисков, основное отличие которых заключается в применяемых шкалах оценивания уровня риска: количественных или качественных [3; 5; 14; 17].

В количественных методиках риск оценивается через числовое значение. В качестве входных данных для оценивания обычно используют накопленную статистическую информацию об инцидентах [6,9]. Однако частое отсутствие достаточного количества статистических данных приводит к снижению адекватности результатов оценивания.

Качественные методики более распространены [2; 7; 8]. Оценивание проводится на основе экспертных опросов, а перспективные интеллектуальные методы пока применяются недостаточно [10].

Исходя из проведенного анализа методик, можно сделать вывод, что большинство из них базируется на эвристических и/или эмпирических подходах, которые не учитывают новых видов угроз для ИИГ, особенно в сфере киберпространства. Большинство из этих методов являются детерминированными, что не учитывает динамику процесса подготовки объектов к началу активной фазы, после наступления которой они могут быть захвачены или нейтрализованы.

Цель статьи. Главная цель этой работы – рассмотрение методических подходов к оцениванию эффективности обеспечения безопасности объектов ИИГ и предлагается формализованная модель функционирования объектов ИИГ.

Изложение основного материала. Такая ситуация вызывает необходимость решения задачи – построение модели функционирования ИИГ, которая учитывала бы неопределенность периода подготовки объектов ИИГ к активной фазе и разнообразие угроз, влияющих на объекты ИИГ.

Исходными данными для создания такой модели будут: показатель уязвимости информационной инфраструктуры государства (Z) – комплексная величина, определяемая как функция (или функционал) ряда факторов, таких как: важность объектов информационной инфраструктуры (W); угроза информационной безопасности (P); потенциально возможный ущерб (R); уязвимость объектов информационной инфраструктуры (U) и время до начала активной фазы (период подготовки объектов к определенному моменту времени) (T).

В предложенной модели подготовка объектов рассматривается как дискретный процесс, созданный множествами параметров ИИГ, в определенные моменты времени $T = \{t_0, t_1, t_2, ..., t_j\}$, с момента, когда начинается подготовка объектов ИИГ (t_0) и к некоторому моменту (t_j), который отвечает моменту начала активной фазы. Сложность определения момента t_j и, соответственно, длительности периода подготовки объектов ИИГ приводит к тому, что нужно стремиться достичь максимального эффекта защиты этих объектов на каждом шаге моделирования. Поэтому главным критерием функционирования такой системы является минимизация уязвимости информационной инфраструктуры государства.

$$Z = f(W, P, R, U, T) \rightarrow \min \qquad (1)$$

Шаг моделирования определяется исходя из длительности периода подготовки объектов к определенному моменту времени tj и должен быть таким, чтобы за это время можно было провести действия по защите объекта, с привлечением внешних средств, или организационными мероприятиями.

Такой подход позволит реализовать принцип естественного эшелонирования защиты и глобальной диверсности.

Основные же сложности анализа угроз связаны с оценкой риска информационной безопасности и его факторов (угроз, возможного ущерба, уязвимостей). Это вызвано следующими проблемами:

1. Неполнотой информации о составляющих риска и их неоднозначные свойства.

2. Сложностью создания модели информационной инфраструктуры и оценивания её уязвимости.

3. Длительностью процесса оценивания и быстрой потерей актуальности его результатов.

4. Сложностью агрегации данных из различных источников, в том числе статистической информации и экспертных оценок.

5. Необходимостью привлечения нескольких специалистов по анализу рисков для повышения адекватности оценивания (как минимум специалистов правоохранительной, технической и кибербезопасности).

Особого внимания заслуживают методы (методики) определения параметров объектов ИИГ, таких как: вес объектов в системе (ранжирование), определение их уязвимостей и мероприятий по нейтрализации деструктивных влияний.

Примером определения степени уязвимости объектов государственной инфраструктуры может служить методика, разработанная министерством внутренней безопасности США. В ее основу положена так называемая модель определения приоритетности объектов основных фондов военно-промышленной базы (The Asset Prioritization Model – (APM)) [16]. Суть ее заключается в расчете индекса рискованности объекта, зависящего от рейтинга объекта по шкале категории факторов и «веса» данного фактора. Методика может быть использована при оценке уязвимости объектов и секторов критической инфраструктуры, в том числе информационной. В этой модели значительно упрощен порядок определения рейтинга объекта с точки зрения оцениваемых параметров – от 1 до 3, где 1 – объект наименее важен, а 3 – объект наиболее важен (в других странах используется 4-х или 5-значный рейтинг).

После описания взаимозависимости объектов критической инфраструктуры ведется поиск наиболее уязвимых из них, воздействие на которые может оказать наиболее негативный эффект на всю инфраструктуру. При этом решается ряд задач, общее количество которых может варьироваться в зависимости от целей исследования и анализируемой ИИГ. Поиском ключевых объектов, воздействие на которые может оказать наиболее негативный эффект, исследование критической инфраструктуры не ограничивается. Это только первый шаг, после чего, как правило, проводится оценивание уязвимости вскрытых «центров тяжести» с помощью метода построения дерева отказов, трансформирующегося в дерево событий, что позволяет определить возможные степени уязвимости инфраструктуры, а также их вариации. Дерево отказов представляет собой бинарное дерево со всеми возможными логическими событиями для каждого потенциального отказа. Именно дерево отказов и событий позволяют сформулировать и разработать возможные мероприятия по защите критических объектов ИИГ.

На следующем этапе разрабатываются алгоритмы оценивания рисков, смысл которых состоит в определении ресурсов, необходимых для обеспечения безопасности наиболее важных из выявленных критических объектов информационной инфраструктуры. При этом одним из главных условий остается соблюдение критерия «стоимость – эффективность», а ключевая проблема состоит в том, чтобы правильно выбрать способы и средства для организации защиты или воздействия [1; 5].

В итоге получаем систему мероприятий по нейтрализации (минимизации) угроз объектам ИИГ и величины возможного ущерба.

При этом основными задачами обеспечения безопасности объектов информационной инфраструктуры должны являться:

1. Систематическое выявление и устранение угроз опасности и их источников.

2. Развитие и совершенствование системы обеспечения безопасности объектов ИИГ, реализующей единую государственную политику в этой области, включая разработку новых и совершенствование существующих способов, методов и средств выявления, оценивания, прогнозирования, нейтрализации и ликвидации угроз, а также средств и методов противодействия этим угрозам.

3. Эффективное противодействие угрозам на объекты ИИГ.

4. Разработка основных направлений государственной политики в области обеспечения безопасности объектов ИИГ, а также мероприятий и механизмов, связанных с реализацией этой политики.

5. Разработка критериев и методов оценивания эффективности системы обеспечения безопасности объектов ИИГ.

6. Совершенствование нормативно-правовой базы по обеспечению безопасности объектов ИИГ.

7. Координация деятельности органов государственного управления в области обеспечения безопасности объектов ИИГ.

8. Разработка научно-практических основ обеспечения безопасности объектов ИИГ.

9. Разработка и реализация целевых программ, направленных на обеспечение безопасности объектов ИИГ.

10. Совершенствование приемов, способов, методов и средств безопасности объектов ИИГ от информационно-технических и информационно-психологических воздействий противоборствующей стороны.

Выводы и предложения. Обеспечение безопасности объектов информационной инфраструктуры должно представлять собой систему мероприятий по деятельности субъектов информационной безопасности по выявлению и ликвидации (нейтрализации) угроз таким объектам, снижению рисков и величины возможного ущерба. Мировой опыт говорит о необходимости создания целостной государственной (межгосударственной) системы защиты ИИГ, сочетающей организационные, оперативные и технические меры нейтрализации различных угроз, которые постоянно развиваются, что требует совершенствования системы защиты ИИГ.

Таким образом, в статье проведен анализ методических подходов к оцениванию обеспечения безопасности объектов информационной инфраструктуры государства, приведено описание формальной модели функционирования объектов ИИГ и рассмотрены принципы определения критических объектов такой структуры и задачи по обеспечению безопасности ИИГ.

Список литературы:

1. Баранник, А., Клементьев С. Организация обеспечения безопасности критической инфраструктуры в США. – М: Зарубежное военное обозрение № 8, 2009. – С. 3-10.
2. Бутусов И.В., Нащекин П.А., Романов А.А. Теоретико-семантические аспекты организации комплексной системы защиты информационных систем // Вопросы кибербезопасности. – 2016. – № 1 (14). – С. 9-16.
3. Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь / Д.С. Бірюков, С.І. Кондратов, О.І. Насвіт, О.М. Суходоля. – К. : НІСД, 2015. – 35 с.
4. Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України. – НІСД. : http://www.niss.gov.ua/articles/1371.
5. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах // Зарубежное военное обозрение. – 2012. – №1. – С. 19-30.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб, пособие для вузов. – М.: Изд-во «Горячая линия-Телеком», 2004. – 280 с.
7. Харченко В С., Одарущенко О Н., Иванченко О.В. Принципы анализа и управления безопасностью критических інфраструктур // Вісник Хмельницького національного університету, 2010, № 5. – С. 218-221.
8. Чукляев И.И. Методика построения и нечеткая модель оценки защищенности и выбора классов мероприятий по минимизации рисков на основе нейронечеткого классификатора // Известия Смоленского государственного университета, 2015. – № 2-1. – С. 312-319.
9. Чукляев И.И. Система комплексной защиты функционально-ориентированных информационных ресурсов информационно-управляющих систем // Системы компьютерной математики и их приложения, 2016. – № 17. – С. 85-88.
10. Шелупанов А.А., Шумский А.А. Системный анализ в защите информации. – М.: Изд-во «Гелиос АРВ», 2005. – 224 с.
11. Beyer. U., Flentge. F.: Towards a Holistic Metamodel for Systems of Critical In¬frastructures. In: ECN CIIP Newsletter, October/November 2006.
12. Casalicchio, E., Galli, E., Tucci, S.: Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures. In: 11th IEEE Symp. on Distributed Simulation & Real-Time App. IEEE Computer Society, Los Alamitos, 2007.
13. Carreras B.A., Dobson I., Newman D.E.: A loading dependent model for probabilistic cascading failure. Probability in the Engineering and Informational Sciences 19, 15–32, 2005.
14. Fast Analysis Infrastructure Tool Department of Homeland Security's Information Analysis and Infrastructure Protection. National Infrastructure Simulation and Analysis Center (NISAC).
15. Inmon W. H. Building the Data Warehouse. – Wiley, 2006.
16. Pederson. P. et al.: Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Technical Report. Idaho National Lab, August 2006.
17. Romani F., Chiaradonna S., Di Giandomenico F., Simoncini L.: Simulation models and implementation of a simulator for the performability analysis of electric power systems considering interdependencies. In: 10th IEEE High Assurance Systems Engineering Symposium (HASE 2007), pp. 305–312, 2007.
18. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT, 2001) : http://frwebgate.access.gpo.gov.

Приймак М.В.
Національний університет оборони України імені Івана Черняховського

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація
У статті проведено аналіз методичних підходів до оцінки ефективного забезпечення безпеки об'єктів інформаційної інфраструктури держави (ІІД). Запропоновано опис формалізованої моделі функціонування об'єктів інформаційної інфраструктури держави. Розглянуто загальні принципи визначення критичних об'єктів інфраструктури. Описана система заходів по нейтралізації (мінімізації) загроз об'єктам ІІД і величини їх можливого збитку. Запропоновано завдання забезпечення безпеки об'єктів ІІД.
Ключові слова: інформаційна інфраструктура держави, критичний об'єкт, інформаційна безпека.

Priymak M.V.
National Defence University of Ukraine named after Ivan Cherniakhovskyi

SECURITY FEATURES THE INFORMATION-INFRASTRUCTURE STATE

Summary
The article analyzes the methodological approaches to evaluating the effectiveness of state security information infrastructure (IIG). A description of a formalized model of the functioning of the information infrastructure of the state. The general principles for the determination of the critical infrastructure. A system of measures to neutralize (minimize) threats facilities IIG and the magnitude of their possible damage. Proposed tasks of security-ing sites IIG.
Keywords: information infrastructure of the state, Cree-matic object information security.